Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

APT28 Leveraged Three Roundcube Exploits in Espionage Campaign

Date of Publication	Admiralty Code	TA Number
June 26, 2023	A1	TA2023278

Summary

Attack Began: May 2023
Actor: APT28 (aka Sofacy, Fancy Bear, Sednit, Group 74, TG-4127, Pawn Storm, Tsar Team, Strontium, Swallowtail, SIG40, Snakemackerel, Iron Twilight, ATK 5, T-APT-12, ITG05, TAG-0700, UAC-0028, FROZENLAKE, Grey-Cloud, Grizzly Steppe, Forest Blizzard, BlueDelta, RON TWILIGHT, Sofacy, Threat Group-4127)
Attack Region: Ukraine
Targeted sectors: Government Institutions, Military, and Media

Attack: APT28 conducted a sophisticated campaign targeting prominent organizations in Ukraine. The campaign involved spear-phishing emails, and these attachments exploited vulnerabilities in the Roundcube webmail platform.

Attack Regions

Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2020-35730	Roundcube Webmail Cross-Site Scripting (XSS) Vulnerability	Roundcube Webmail	✗	✓	✓

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2021-44026	Roundcube Webmail SQL Injection Vulnerability	Roundcube Webmail	✗	✓	✓
CVE-2020-12641	Roundcube Webmail Remote Code Execution Vulnerability	Roundcube Webmail	✗	✓	✓

Attack Details

#1 A campaign conducted by APT28, also known as BlueDelta, focused on various prominent organizations in Ukraine. This operation involved correlating a spearphishing campaign with the use of news related to Russia's conflict with Ukraine. The objective was to entice recipients into opening emails while exploiting vulnerabilities in Roundcube servers, which are open-source webmail software.

#2 This tactic enabled the execution of multiple reconnaissance and exfiltration scripts. Considering the targeted entities, the geopolitical context, and the group's organizational connections, it is highly probable that the highlighted APT28 activity aimed to facilitate military intelligence gathering in support of Russia's invasion of Ukraine. The spearphishing email associated with this APT28 campaign included a JavaScript file attachment.

#3 This attachment was specifically designed to exploit an XSS Vulnerability (CVE-2020-35730), targeting users of the Roundcube webmail platform. Once the exploitation occurs, the JavaScript code retrieves and executes additional JavaScript files named "q.js" and "e.js" from a remote server. It is important to note that the exploit can occur without any interaction between the victim and the attachment, apart from opening the email.

#4 Within the mentioned files, "e.js" creates a "default filter" that redirects incoming emails to a third-party email address while facilitating exfiltration through HTTP POST requests. The exfiltrated data includes the address book, session values, and the victim's emails. On the other hand, "q.js" contains an exploit for the Roundcube SQL Injection vulnerability (CVE-2021-44026), enabling the extraction of information from the Roundcube database.

#5 Additionally, the code "c.js" was discovered, which exploits the Remote Code Execution vulnerability (CVE-2020-12641) in Roundcube, allowing for the execution of commands on the mail server. It is worth noting that APT28 previously exploited a zero-day vulnerability in Microsoft Outlook (CVE-2023-23397) to target the Ukrainian civic community.

Recommendations

Patch and update the Roundcube webmail platform to address vulnerabilities such as XSS (CVE-2020-35730), SQL Injection (CVE-2021-44026), and Remote Code Execution (CVE-2020-12641), to prevent APT28's exfiltration and command execution activities.

Enhance email security measures, including user awareness training on identifying and avoiding spearphishing emails, to mitigate the risk of APT28's exploitation of vulnerabilities and the exfiltration of sensitive information from the Roundcube database.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0005** Defense Evasion	**TA0006** Credential Access
TA0007 Discovery	**TA0009** Collection	**TA0011** Command and Control	**TA0010** Exfiltration
T1566 Phishing	**T1566.001** Spearphishing Attachment	**T1203** Exploitation for Client Execution	**T1027** Obfuscated Files or Information
T1059 Command and Scripting Interpreter	**T1059.007** JavaScript	**T1140** Deobfuscate/Decode Files or Information	**T1003** OS Credential Dumping
T1003.008 /etc/passwd and /etc/shadow	**T1082** System Information Discovery	**T1016** System Network Configuration Discovery	**T1033** System Owner/User Discovery
T1049 System Network Connections Discovery	**T1114** Email Collection	**T1114.003** Email Forwarding Rule	**T1071** Application Layer Protocol

T1071.001 Web Protocols	**T1132** Data Encoding	**T1132.001** Standard Encoding	**T1048** Exfiltration Over Alternative Protocol
T1020 Automated Exfiltration			

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	a723e1a8231023d14925bcf1eb84667b f3bb09a022e99fd556dd2bdf15f46ff0 9e2926d1237b24e33db655041fd60ebf 6e17139a83b062ce90042a8c56b59f48 0c030fe8696b00600baf8653c507cb80
SHA256	d94b13e70e97053e2171ddb81c749f90959ad90ea415b839be34ff78fc9bed4d d4513d9c26cf8040bce4bbebefb8a2dcc2d35fc92d79083879b1f274d17ab197 d6899f318026b65342d74682bab64d50da9fe8fb31a2765d99015b5aeb025e7a fed8487faa22fe2fc1d3580d2028de44e7a274a8e22981dbf96346f5f74171d8 1277be4f8ef5af3404487f49a5ca3d0e506e64b24eebcfa65f196f983f6c4f11
Email Addresses	ukraine_news[@]meta[.]ua str.vidil[@]meta[.]ua
IPV4	5[.]199.162.132 185[.]225.226.57 185[.]82.126.85 77[.]243.181.238 46[.]183.219.207 144[.]76.69.94 46[.]183.219.232 45[.]138.87.250 144[.]76.7.190 77[.]243.181.10 185[.]210.217.218 144[.]76.184.94 162[.]55.241.4 185[.]195.236.230

TYPE	VALUE
URLs	hXXps://global-world-news[.]net:443/about/<base64_string> hXXps://global-world-news[.]net:443/addressbook/<base64_string> hXXps://global-world-news[.]net:443/db/<base64_string> hXXps://global-world-news[.]net:443/e?m=<base64_string>&r=<base64_string_2>&s=<base64_string_3> hXXps://global-world-news[.]net:443/e?m=<base64_string>&r=<base64_string_2>&s=<base64_string_3> hXXps://global-world-news[.]net:443/emails/<base64_string> hXXps://global-world-news[.]net:443/l/<base64_string> hXXps://global-world-news[.]net:443/q?r=<base64_string_2>&m=<base64_string> hXXps://global-world-news[.]net:443/q?r=<base64_string_2>&m=<base64_string> hXXps://global-world-news[.]net:443/s/<base64_string>
Domains	aneria[.]net global-news-world[.]com global-world-news[.]net armpress[.]net ceriossl[.]info newsnew[.]info globalnewsnew[.]com sourcescdn[.]net runstatistics[.]net mai1[.]namenews[.]info starvars[.]top infocentre[.]icu fountainrate[.]com lonejade[.]com modeselling[.]com oncetrips[.]com vtxhospital[.]com ns1.fountainrate[.]com ns2.fountainrate[.]com ns1.lonejade[.]com ns1.modeselling[.]com ns2.modeselling[.]com ns1.oncetrips[.]com ns2.oncetrips[.]com ns1.vtxhospital[.]com ns2.vtxhospital[.]com

Patch Links

https://roundcube.net/news/2020/12/27/security-updates-1.4.10-1.3.16-and-1.2.13

https://roundcube.net/news/2021/11/12/security-updates-1.4.12-and-1.3.17-released

https://roundcube.net/news/2020/04/29/security-updates-1.4.4-1.3.11-and-1.2.10

References

https://go.recordedfuture.com/hubfs/reports/cta-2023-0620.pdf

https://cert.gov.ua/article/4905829

https://www.hivepro.com/apt28s-cyber-espionage-campaigns-targeting-ukraine/

https://www.hivepro.com/apt28s-snmp-attack-on-cisco-routers/

https://attack.mitre.org/groups/G0007/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.

Contextualize
Uni5 Threat Exposure Management
Prioritize
Resolve

REPORT GENERATED ON

June 26, 2023 • 5:00 AM

More at www.hivepro.com